



**School of
Management and Law**

Cyber Risks and Swiss SMEs

**An investigation of employee attitudes and
behavioral vulnerabilities**

**Carlo Pugnetti, ZHAW Institute for Risk & Insurance
Carlos Casián, Allianz Suisse**

In cooperation with:



Publisher
ZHAW School of Management and Law
St.-Georgen-Platz 2
P.O. Box
8401 Winterthur
Switzerland

Institute for Risk & Insurance (IRI)
www.zhaw.ch/en/sml/institutes-centres/iri/

Author/Contact
Dr. Carlo Pignetti
carlo.pignetti@zhaw.ch

January 2021

Copyright © 2021,
ZHAW School of Management and Law

All rights reserved. Nothing from this publication
may be reproduced, stored in computerized systems,
or published in any form or in any manner, including
electronic, mechanical, reprographic, or photographic,
without prior written permission from the publisher.

Editorial

The evolution and widespread adoption of technology is opening new and exciting ways to improve our lives with better products and services as well as better and more frequent human contact. Unfortunately, these changes also present criminals with new opportunities. We know from experience that these adversaries can be intelligent, well-equipped and creative, and they will find and take advantage of any technological or human weakness in our defenses. These developments are also significant for insurers underwriting these emergent risks.

The issue is especially critical for small and medium enterprises (SMEs) in Switzerland, who are often at the leading edge of market development and innovation but have limited resources to devote to cyber security. The last few years have demonstrated just how much these companies are in the crosshairs of cyber criminals. At Allianz Suisse, we have always supported our customers with excellent products, tailored services, and ground-breaking solutions, and this new study is in keeping with our record of innovation.

The attitude of employees towards cyber risks is a critical component of a company's overall protection and response mechanism. The Zurich University of Applied Sciences (ZHAW) has developed an exciting research focus on customer behavior in insurance, and we are glad to be associated with this research. This study, in particular, has identified interesting behavioral and cultural insights into SME employee attitudes and developed clear and insightful recommendations for the companies themselves as well as for their technology and insurance providers.

I hope you will find this publication both informative and thought-provoking.

Severin Moser

CEO, Allianz Suisse

Management Summary

Cyber attacks are an increasingly significant issue for Swiss SMEs. About one third have already experienced cyber attacks, and four percent have been blackmailed as a result. Most of these problems began with phishing attacks, where criminal elements gained access to the IT system by exploiting an employee error or oversight. We interviewed several employees of Swiss SMEs to understand how their attitudes towards cyber attacks may affect this vulnerability and to develop practical suggestions for corrective action. The interviews were conducted using deep metaphors to understand the hidden cultural and emotional drivers of behavior rather than the rational, visible components. We developed three recommendations to take advantage of the proactive culture at SMEs and decrease their dependence on third-party providers: raise awareness, empower employees, and train a recovery mode.

Table of Contents

Editorial	3
Management Summary	4
Table of Contents	5
Introduction	6
1.1. Cyber Risks and the Swiss SME	6
1.2. Examples of Prominent Cyber Attacks in Switzerland	7
1.3. Protecting Your Company	9
1.4. Deep Metaphor Interviews	10
1.5. Methodology	11
Results	12
2.1. Global Politics and Organized Crime	13
2.2. The Mythical Hacker	14
2.3. Feeling Helpless	15
2.4. Feeling Vulnerable	16
2.5. Catastrophic Outcome	17
2.6. It Does not Concern Me	18
2.7. Proactive and Engaged	19
Discussion	20
3.1. Impact by Employee Category	20
3.2. Recommendations for Improvement	21
Conclusions	23
References	24
Tables	28
Figures	29
Authors	30
Partners	31

Introduction

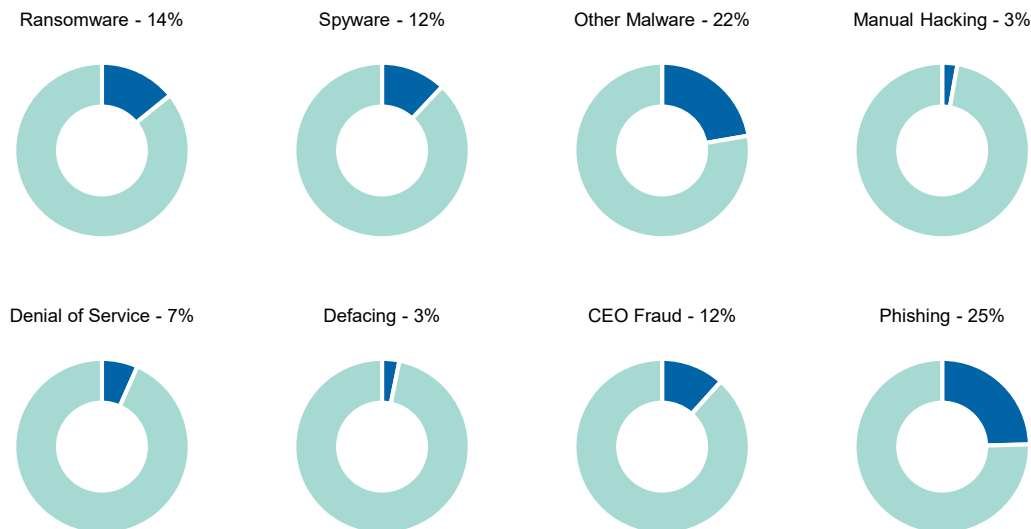
1.1. CYBER RISKS AND THE SWISS SME

Data or security breaches, espionage, hacker attacks, ransomware, denial of service, and employee errors are the leading causes of cyber incidents, and they are becoming more common and increasingly costly. This development is reflected in the Allianz Risk Barometer (2020), to which more than 2,700 risk experts worldwide contributed: Cyber incidents have displaced business interruption as the top risk. The increasing interconnectedness of the economy means that companies are becoming more vulnerable to cyber attacks, and reports of spectacular hacker attacks and data thefts are growing. Companies are threatened with damages running into millions, the loss of image, and even a business interruption that threatens their existence if cyber criminals steal data, smuggle malicious programs into networks, or paralyze servers (Allianz, 2020). Severin Moser, CEO at Allianz Suisse, estimates that the consequences of cyber crime cost the global economy more than US\$ 600 billion per year (NZZ, 2019). However, it is difficult to quantify the development in detail due to a lack of reliable figures and many unreported cases. The Cyber Risk Working Group at the Swiss Insurance Association estimates the annual cost in Switzerland alone to be CHF 9.5 billion, and the figure is rising (SIA, 2018).

Small and medium-sized enterprises (SMEs), defined as companies employing up to 250 people, make up more than 99% of companies and provide two-thirds of the jobs in Switzerland (Federal Statistical Office, 2020). They play a crucial role in the Swiss economy and are heavily affected by cyber attacks. About a third of Swiss SMEs have already experienced cyber attacks, and some four percent have been blackmailed as a result of these attacks (Mändli Lerch and Repic, 2017). Even if the data from smaller companies are of little interest to cyber criminals, these companies remain attractive targets for two reasons: First, for extorting a ransom using ransomware, and second, as a gateway for attacking larger companies working with the SMEs (Heer, 2020). The Reporting and Analysis Center for Information Assurance, which was integrated into the National Center for Cybersecurity (NCSC) in July 2020, reported an increased risk from ransomware attacks in early 2020 (MELANI, 2020a). This threat continues to grow, and having quadrupled in 2019, it is now the most common cyber incident (Trustwave, 2020). There are numerous examples of Swiss companies falling victim to ransomware attacks, and four of them are discussed in the following chapter.

Recent studies have started to look at cyber attacks on SMEs in more detail in neighboring countries. Dreissigacker et al. (2020) estimate that in Germany, for example, 40 to 50 percent of SMEs with more than ten employees are exposed to a cyber attack each year, even if most of these attacks are neutralized and do not cause any harm. This figure is lower, though not significantly, than that for larger companies, which are attacked at a rate of 50 to 60 percent per year. This study further investigates the yearly rate for each major category of cyber attack, as summarized in Figure 1. SMEs can expect a phishing attack every four years and a ransomware attack every seven, roughly in line with the rates for larger companies. On the other hand, CEO fraud attacks and manual hacking are significantly lower for SMEs, perhaps due to the more hands-on role of the CEO in smaller companies and the potentially lower financial gain. Studies in other European countries report similar results but sometimes with significant deviations, though a direct comparison is difficult because of different research methodologies and reporting mechanisms. In general, however, they confirm a substantial overall threat to SMEs from cyber attacks.

Figure 1: Estimated yearly rate of cyber attacks on SMEs

ESTIMATED RATE OF CYBER ATTACKS ON SMES PER YEAR BY TYPE IN GERMANY 2018/2019

Source: Dreissigacker et al. (2020)

Malevolent cyber actors regularly adapt social engineering attacks, especially phishing, to current major events such as sports events or the current COVID-19 pandemic. However, practically all common malware families have been spread with a COVID-19 pretext, most commonly using emails with a contaminated attachment or a link to an infected website (MELANI, 2020b). The number of phishing emails has soared during the pandemic; for example, scammers impersonating World Health Organization (WHO) employees have targeted relief funds for COVID-19 victims and lured users to malicious websites using fake advertisements (de Moura et al., 2020). Phishing attacks have also been aimed specifically at the changed work environment. Many users were initially unfamiliar with conference and collaboration software, and the messages sent by these platforms, making phishing emails more difficult to recognize (MELANI, 2020b). Several articles identify the vulnerabilities of companies due to human error and the significance of phishing attacks. While the technical infrastructure remains critical, employees often fall prey to cleverly devised schemes and expose their companies to fraud or malware (Pugnetti et al., 2019). Swiss SMEs are generally under-protected against cyber risks, especially concerning services for mitigation and recovery (Pugnetti and Schneebeili, 2020).

This research aims to understand potential vulnerabilities due to employee perceptions of cyber crime and SME company culture and to develop suggestions for coping mechanisms for use by companies as well as training and services that can be provided by third parties.

1.2. EXAMPLES OF PROMINENT CYBER ATTACKS IN SWITZERLAND

There have been several cases of cyber attacks against Swiss SMEs reported in the media. Four attacks were particularly relevant for the companies interviewed in this study and are described below in some detail.

1.2.1. OFFIX AG, 2019

OFFIX AG, which operates in the office equipment sector, employing some 250 people and with a turnover of CHF 300 million (Papedis, n.d.), was the victim of a ransomware attack on 15 May 2019 (Jochum, 2019). It is assumed that a hacker intercepted email correspondence with a customer and substituted the customer in the exchange. A company employee then received a certification request, clicked on the link provided, and the virus infected the company's IT system. The first irregularities became apparent a day later, and, on 17 May, it became clear that in terms of IT, there was "nothing left": databases had been deleted and numerous servers restored to factory settings. Many customer interfaces for order placement were also deleted, and OFFIX lost track of incoming orders and sales. A ransom of 45 bitcoins (at the time valued at CHF 350,000) was demanded for decryption. An external cyber

crime specialist was engaged, and the federal Reporting and Analysis Center for Information Assurance (MELANI) as well as the police were informed. Customers were then asked to place further orders via telephone, fax, or newly set up email addresses before the entire company went offline. Fortunately, the hacker had made a mistake, and, in addition, an important application had been saved on an external hard drive by an IT specialist only a few weeks previously. As a result, OFFIX managed to restore part of its database and could then rebuild its IT systems (Severin, 2019). According to the CEO, Martin Kelterborn, the financial damage could not be quantified, but the attack was “very, very expensive” (Jochum, 2019).

1.2.2. Swisswindows, 2019

In May 2019, Swisswindows, a window fitter with around 170 employees (Borkert, 2020), endured a production downtime of over a month due to a ransomware attack. Hackers had probably gained access to the company network through an inconspicuous email and encrypted all the company’s data. Orders were no longer visible, and employees had no access to customer and machine data. The company was paralyzed. An external IT company had run daily data backups, but the backup files were attached to the company server and were therefore also inaccessible. Although the cyber criminals demanded a large ransom in bitcoins to release the data, the company decided not to pay the ransom but to invest in replacing its IT infrastructure, which was necessary anyway (Klein, 2020). However, in February 2020, the workforce was unexpectedly informed that the company was bankrupt. The cyber attack had further exacerbated an ongoing decline in the company’s core business activities and was, therefore, a contributing factor to its downfall (SRF, 2020).

1.2.3. Meier Tobler, 2019

Meier Tobler, the building technology company, with revenues of CHF 500 million and some 1,300 employees (Meier Tobler, 2020), suffered a ransomware attack in July 2019 (Luzerner Zeitung, 2019). Attackers gained access through an email attachment containing malware (Schäppi, 2020). The central SAP system, the warehouse control system, landline telephony, the website, and all email addresses stopped working (Lüscher and Niedermann, 2019). This had a significant impact on sales and profits as per the company’s press release:

Although the prepared emergency procedures took effect and a provisional infrastructure could be set up within a short time, a temporary interruption in deliveries could not be prevented. This resulted in an immediate drop in sales in the trading business of around CHF 5 million. An additional loss of sales of a similar magnitude occurred later in the heat generation business due to the lack of availability of the IT systems.

The direct extra cost of coping with the attack affected 2019 annual profits by CHF 1 million. The company has since rebuilt its IT infrastructure in accordance with the latest security criteria (Meier Tobler, 2020).

1.2.4. Stadler Rail, 2020

Stadler Rail manufactures rail vehicles, and with 11,000 employees and global revenues of over CHF 3.2 billion (Stadler Rail, 2020a), it is not an SME. However, this cyber attack was mentioned by people interviewed for this study, and it is therefore relevant. On May 7, 2020 “The Stadler IT network was attacked with malware. The company has immediately initiated the required security measures and it has involved the responsible authorities. A detailed investigation of the matter is ongoing.” (Stadler Rail, 2020b). The perpetrators blackmailed Stadler with the publication of stolen data and demanded payment of six million US dollars in bitcoin. The company confirmed in a statement to inside-it.ch that “These are confidential documents and data that were stolen from Stadler through criminal activities” (Anz, 2020). Stadler refused to pay the ransom, and some records were published to increase pressure, followed by the publication of more records as the company continued to refuse payment (Griesser Kym, 2020). However, Stadler was at no time ready to respond to the demands of the blackmailers and make payments - and “will not do so” (Anz, 2020).

1.3. PROTECTING YOUR COMPANY

All companies need to determine what risks they want to avoid, mitigate, transfer, or bear themselves as part of their risk management decision process. In this context, it is crucial to understand what insurance solutions are available to them and would have provided some level of protection in the cases described above. Cyber attacks can cause first-party losses, such as restoration costs for data, and interrupt regular business operations. Standard property insurance policies cover property damage and the resulting business interruption if the cause of the damage (e.g., a fire) is insured. However, property damage does not necessarily occur in the event of a cyber attack, and it is therefore rare for property insurance to be invoked. Furthermore, companies may be confronted with third-party liability claims after a cyber attack if, for example, customer data is leaked or deleted. Conventional third-party insurance covers liability claims from personal injury and property damage and the resulting financial loss. Third-party liability insurance covering a purely financial loss is usually only intended for specific professional groups and is, therefore, not widespread.

The established, classic commercial insurance policies have one thing in common: they do not specifically address cyber risks. Under certain circumstances, the damage and effects of a cyber attack are insured through such products, but they are not explicitly designed to make cyber risk controllable for companies. It should be noted that cyber risks did not arise until the internet age, and the first cyber risk coverages were created around the turn of the millennium to address this new threat. In Switzerland, the first cyber risk policies were introduced by international insurers of large companies in 2015, and comprehensive insurance solutions for SMEs were launched in 2017. They usually contain third party liability, first-party losses, and crisis management, and also cover cyber crime / social engineering and cyber risk legal protection. The focus of these products is on cyber attacks as well as employee misconduct and data protection violations. In addition to paying for the damages incurred, companies receive access to a network of specialists in information technology, crisis communication, and legal protection to determine the extent of the damage, speed up damage repair, and avoid or mitigate damage to the company's reputation. Table 1 provides an overview of currently available and customary cyber insurance coverages (Pugnetti et al., 2019).

Table 1: Current cyber insurance coverages

CURRENT CYBER INSURANCE COVERAGES

Third-party liability Claims and demands from third parties	<ul style="list-style-type: none"> - Data protection breaches - Loss of data - Misappropriation/loss of functionality - Digital communication - E-payment/contractual penalties - Forwarding of malware
First-party losses Losses incurred by the policyholder	<ul style="list-style-type: none"> - Restoration costs - Business interruption - Theft by cyber attack - Cyber blackmail - Official data protection procedures
Crisis management Services in the event of a claim	<ul style="list-style-type: none"> - Forensic services - Information costs - Crisis communication - Emergency costs
Legal protection Disputes in connection with cyber risks	<ul style="list-style-type: none"> - Contract law - Violation of personality rights - Misuse of identity - Misuse of credit cards and account information - Internet domain
Cyber crime - Social engineering Financial losses due to deception by a third party	<ul style="list-style-type: none"> - Fraud through the assumption of a false identity - Fraud through the diversion of cash flows - Fraud through the use of fake identities

1.4. DEEP METAPHOR INTERVIEWS

Consumer research has long focused on understanding cognitive structures, i.e., belief systems and emphasizing structure over content (Olson and Reynolds, 1983). However, a better term to describe and represent consumers is the mental model, which allows for non-belief-based representations, including attitudes, feelings, images, memories, values, etc. (Christensen and Olson, 2002). This is also more in line with the current cognitive neuroscience view that sees thoughts as image based (Damasio, 1994). Research and elicitation tools have evolved to attempt to capture the additional complexity of mental models – one of which is the Zaltman metaphor-elicitation technique (ZMET). The theoretical assumption underlying ZMET is, in particular, the importance of unconscious tacit content, i.e., hidden knowledge and the importance of images in mental models. ZMET uses pictures to help informants identify and communicate content (Zaltman, 1997) and has been used to elicit the deeper emotional drivers of behavior and choice among consumers (Zaltman and Zaltman, 2008).

The technique is based on three stages. First, respondents are asked to think about a topic and select pictures representing their thoughts and feelings on the topic. They are then interviewed to understand the meanings they assigned to the images, and connections to superordinate ideas are established using laddering probes. Finally, the findings are generated by creating consensus maps of central constructs and broad themes of meaning (Christensen and Olson, 2002). The final result is a set of themes that interviewees associate with the topic being researched. There is no attempt to generate statistically significant results; instead, the focus is on bringing hidden insights to the surface. The technique has been used in several studies, including by the authors of this study for consulting projects and in a published study to investigate the experience of new insurance customers. In that study, for example, new customers clearly signaled their frustration with the industry's technical jargon and their lack of familiarity with insurance brands (Pugnetti and Bekaert, 2018).

1.5. METHODOLOGY

We recruited three SMEs with activities related to mechanical engineering and conducted deep metaphors interviews with 17 volunteers across a broad cross-section of employee profiles in the organization, including management, administrative staff, shop floor, and field employees. Interviewees were asked to select 3-5 pictures describing how they felt when they heard reports of cyber attacks (Table 2). They were then interviewed about the meaning of the images chosen.

Table 2: Research question

Research Question	How do you feel when you hear about cyber attacks?
-------------------	--

The interviews were conducted in September 2020 jointly by both authors and at each of the company premises. These lasted approximately one hour each, depending on the number of pictures used and the follow-up questions triggered by the discussion. The results were then discussed in a series of workshops and consolidated to generate the consensus maps and main themes presented. These themes are discussed in the following sections using the original pictures and language from the interviews. In a few instances, original images were replaced with similar pictures due to licensing issues.

The interviewees described themselves as summarized in Table 3:¹

Table 3: Self-description of interviewees

SELF-DESCRIPTION OF INTERVIEWEES

1	Helpful, does not want to hurt anybody	10	Friendly, cares about others
2	Person with positive outlook	11	Open but careful
3	Quiet and thoughtful	12	Grounded but open
4	Happy with life	13	Cautious
5	Quiet, does not look for trouble	14	Good-natured, flexible
6	Loyal, good listener	15	Conservative but open
7	Positive person	16	In charge
8	Goal-oriented	17	Communicative and curious
9	Quiet and dependable		

¹ To preserve confidentiality, the order does not correspond to the order of the interviews

Results

The interviews revealed several common threads. One repeated theme was the geopolitical nature of cyber attacks, links to organized crime, and the financial motivation. The hacker was seen as a “professional” with expert skills and excellent equipment, and not necessarily always a force for evil. In general, interviewees felt helpless to recognize cyber attacks or protect themselves. Consequently, they felt vulnerable yet aware of the dangers posed by phishing attacks, and appreciated the potentially catastrophic outcome of cyber attacks. Many mentioned the recent case at Meier Tobler. At the same time, they felt they were not important enough, nor their company large enough, to be targeted. In case of an emergency they would rely on external service providers to solve the problem. Finally, they revealed a very positive attitude towards problem-solving and finding solutions independently, including resorting to old-fashioned methods if necessary.

Table 4: Common themes and picture labels

THEME	PICTURE LABELS
1 Global Politics and Organized Crime	Secret service Man in the shadow The loot
2 The Mythical Hacker	The hacker Cool working space Villain or benefactor?
3 Feeling Helpless	Data magnet Social manipulation Unanswered questions
4 Feeling Vulnerable	Surveillance Be careful! Phishing
5 Catastrophic Outcome	Modern breaking and entering Attack on our supplier I hope not!
6 It Does Not Concern Me	The whole world Fear Personal support
7 Proactive and Engaged	Fog Planning Like in the old days

These nuanced and multi-faceted responses to a relatively straightforward question indicate sophisticated thinking. This enabled the identification of several areas for improvement and the development of clear recommendations for Swiss SMEs and their service providers.

2.1. GLOBAL POLITICS AND ORGANIZED CRIME

Cyber attacks were seen as part of a pattern of international intrigue and high-stakes, global, political games. Although several interviewees could name cyber attacks close to them or their company (overwhelmingly Meier Tobler, as discussed earlier), they generally placed cyber attacks in the context of international political confrontations. The US election and suspected Russian interference were often cited as examples, as was terrorism. Switzerland, however, was considered a safe haven, with a more stable political system. However, interviewees were aware that organized crime is a powerful and coordinating force behind cyber attacks. Successful attacks need the broad coordination of several specialists and data sources over time, requiring organization. Financial gain was identified as a driver of cyber attacks, with a desire for power occasionally mentioned. While the political component may make cyber crime seem relatively more remote, financial and criminal motives bring it closer, making it more recognizable and therefore more relevant to interviewees.

Figure 2: Secret service



SECRET SERVICE

There are large shifts in the international power structure, and it is not so important if a few people die. Things are different in Switzerland, though, the whole system is safer.

Figure 3: Man in the shadow



MAN IN THE SHADOW

It is not known who the person is, but it is clearly organized crime, the mafia. One can call the police or get out of the way, but it is too dangerous to confront him directly.

Figure 4: The loot



THE LOOT

Money, a lot of money. At the end of the day the whole thing is about money.

The tendency to associate cyber crime with large geopolitical forces while assuming Switzerland is a safe haven may make Swiss SMEs vulnerable. Employees may not be as alert as they should be. However, recognizing the role of organized crime and its associated financial motives is a positive sign.

2.2. THE MYTHICAL HACKER

The person carrying out the actual attack was often referred to with the English word “hacker” and depicted as a hooded figure behind a computer. All interviewees indicated that a hacker would most likely not actually look like this and could be male or female. Hackers were seen as having considerable technical expertise and benefiting from well-equipped work spaces - better, in fact, than any of their intended victims. Hackers were not universally seen as a force for evil. Often they were identified as potential force for good – exposing pedophile rings and or corruption, for example. This differentiated view of hacking opens the door for ethical hackers to probe a company's defenses in return for legitimate remuneration.

Figure 5: The hacker



THE HACKER

*Connected with several people in several countries.
Anonymous and frightening.*

Figure 6: Cool working space



COOL WORKING SPACE

I don't know why he has so many devices, but he uses all of them. He can even hack companies that are prepared and well protected.

Figure 7: Villain or benefactor?



VILLAIN OR BENEFACTOR?

I feel neutral about it. Could be a criminal or a whistleblower.

Interviewee responses confirmed an awareness of the complicated nature of cyber attacks and what drives them, as well as the potential benefits of whistleblowing activity. However, by linking attacks to larger geopolitical forces, they risk relegating cyber attacks to a context where they and their SMEs are “too insignificant” to attract unwelcome attention – automatically raising their vulnerability.

2.3. FEELING HELPLESS

Interviewees spoke openly about the opaqueness of cyber attacks and their lack of understanding of the dynamics. Data can be mined without anyone noticing, like a magnet attracting ferrous metals. Attitudes towards cyber attacks can be influenced and manipulated over time without anyone noticing. Several questions are left unanswered - who is behind the attacks and why, and how you should react during or after an attack. The current, overall feeling is one of helplessness towards cyber attacks. This is not a positive sign, because it discourages active involvement and taking sensible defense measures. On the other hand, information campaigns and training programs to improve knowledge and awareness should find an interested and motivated audience.

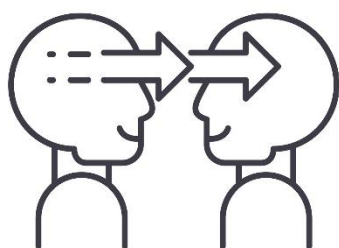
Figure 8: Data magnet



DATA MAGNET

Data can be pulled out of a network like a magnet that pulls everything towards itself.

Figure 9: Social manipulation



SOCIAL MANIPULATION

Trust is being abused. If an employee is not paying attention they can make a mistake and can lose their job.

Figure 10: Unanswered questions



UNANSWERED QUESTIONS

Why did he do that? What can we do? We cannot provide any answers or find any solutions by ourselves.

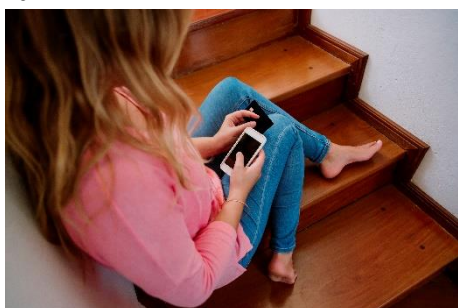
Unfortunately, a feeling of helplessness triggers passivity, both in preparation for and in response to a cyber attack. Responsibility for cyber protection then shifts to more knowledgeable specialized third parties, rather than maintaining the focus on every employee's role in safeguarding the company. Dedicated training programs need to be developed to raise awareness of risky behavior and knowledge of the tools available to make employees more proactive.

2.4. FEELING VULNERABLE

Interviewees know that they are being watched when they are online. They do not like the feeling, and they do not like their inability to prevent themselves from being observed. They know that their trust can be abused to harm the companies they work for and that they can suffer directly or indirectly from this. One interviewee compared this to opening the door for an unknown person, who could then enter the building and steal equipment. In addition, we all have private lives and behaviors that we would not be proud of if they were made public or shared with a wider audience. This makes us vulnerable and unable to defend ourselves against an attack. Hackers exploit our vulnerability and gain access through phishing attacks designed to catch us off our guard.

This feeling of vulnerability is unpleasant, and one common human reaction is to avoid thinking about it. As one interviewee said, “if we thought about all that could happen, we would never go online.” However, an awareness of the seriousness of phishing attacks is an encouraging indication of the level of knowledge employees already possess concerning cyber attacks and, therefore, a useful point of reference in training sessions.

Figure 11: Surveillance



SURVEILLANCE

Somebody is looking over this young woman's shoulder. She cannot prevent it. I do not like it when I have this feeling.

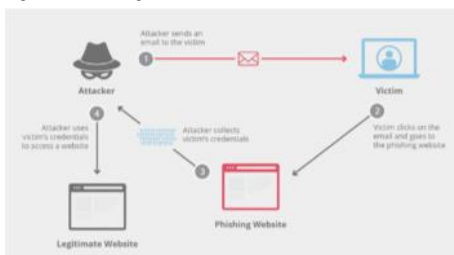
Figure 12: Be careful!



BE CAREFUL!

This person is being blackmailed – something in his private history has been made public. He made a mistake on a social media platform.

Figure 13: Phishing



PHISHING

Data are stolen through phishing attacks. You can try to protect yourself with antivirus and other programs, but that will not protect you against professionals.

An awareness of being observed is a positive sign and can motivate a greater appreciation of risks and a more cautious approach when online. An understanding of the specific threat posed by phishing is significant and encouraging. Phishing is the most insidious way to exploit human vulnerabilities because it collects information and allows attackers to operate unseen and for a considerable time before striking. Effective measures to tackle phishing will need to involve educating people to respond to online requests with the appropriate caution.

2.5. CATASTROPHIC OUTCOME

Respondents viewed cyber attacks as just another form of breaking and entering, and, like its physical counterpart, even an unsuccessful attempt is damaging and unsettling. The incident that crippled Meier Tobler, a supplier, raised awareness of the potentially catastrophic outcome of such an attack. While the company was eventually able to restore operations, the financial damage was significant, and the interviewees themselves were impacted in their daily business. Interestingly, while showing full support and understanding of their business partner's problems, there was evident irritation and shortage of patience that the issues could not be resolved sooner. In general, there was a strong awareness of the potential for IT systems to be paralyzed and of the catastrophic impact this would have on the business.

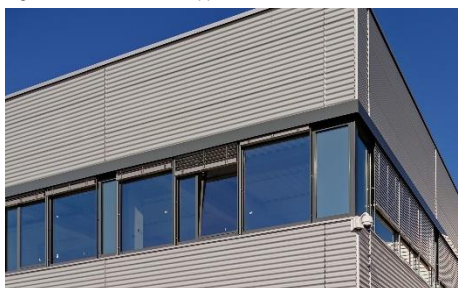
Figure 14: Modern breaking and entering



MODERN BREAKING AND ENTERING

Cyber is just a modern form of entering someone's home. The normal protection is not enough to stop people from breaking in and there are damages regardless of what happens – at least a broken window.

Figure 15: Attack on our supplier



ATTACK ON OUR SUPPLIER

Our supplier was fully automated and was attacked. It could no longer function and lost millions. The same thing might happen to us too.

Figure 16: I hope not!



I HOPE NOT!

The whole thing can blow up in our faces.

The awareness of the potential consequences of cyber attacks provides a clear entry point for training programs. It was also evident that goodwill towards trading partners affected by cyber attacks was limited, indicating that the recovery window before a long-term impact on the business relationships may be relatively short. In the event of an attack, it is therefore vital to restore business operations as swiftly as possible.

2.6. IT DOES NOT CONCERN ME

While interviewees recognized their individual vulnerabilities, they also considered themselves of limited value and, therefore, unlikely to attract unwanted attention. To some extent, this thinking also applied to the company in which they worked. SMEs were viewed as too small when compared to multinationals. The interviews also revealed an underlying feeling that the dangers could be overstated and that fear of attack might prompt unnecessary and possibly detrimental protective action. However, if the company were attacked, external service providers would provide solutions and expertise to tackle the problem, in much the same way as good nurse in a well-equipped hospital treats sick patients. This comparison, in particular, suggests a potential systemic weakness. We readily place ourselves in the care of doctors and nurses and would not self-medicate if we were seriously unwell. Similarly, we may assume it is automatically better to leave digital security solely in the hands of specialists.

Figure 17: The whole world



THE WHOLE WORLD

As soon as the plug goes in, the whole world is connected and we have access to the all the knowledge. A very positive change.

Figure 18: Fear



FEAR

Unfounded fear of anything happening online, although we are relatively safe. Too much protection is not necessary.

Figure 19: Personal support



PERSONAL SUPPORT

This is how a company feels when it's under attack – like somebody who is sick and needs external experts and specialized equipment to be treated.

The notion of being too small and insignificant to be targeted by cyber criminals is perhaps the most worrying aspect of how many SME employees think. While individuals may not be the ultimate target of an attack, they can unwittingly be the weakest link in the chain if cyber criminals can access a company's systems through them. Small SMEs may not be in the direct line of fire, but they can still be targets of opportunity for criminals. Over-reliance on third-party expertise may also shift the problem and its solution away from individual responsibility, further limiting awareness and responsiveness in the event of a cyber attack.

2.7. PROACTIVE AND ENGAGED

When discussing potential attacks and operational disruptions, interviewees demonstrated a remarkable range of reactions. Rather than being paralyzed, they displayed their enthusiasm for tackling the problem and moving forward. Thus a foggy road - signaling limited information - became a metaphor for finding the right path in spite of the adversity, and a blank road sign became the symbol for the need to develop a solution. Multiple tools based on older technologies and workflows can be utilized to keep the company operating in case of a disruption.

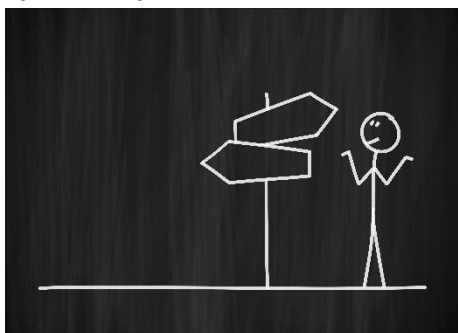
Figure 20: Fog



Fog

During cyber attacks everything is unclear, but I want to move forward along the path, find the way to a solution. I am not scared by what is hiding in the fog, but have to move carefully in order to not lose the path.

Figure 21: Planning



PLANNING

You have to label the signs yourself, and there is no standard solution. The signs point in different directions because you can always have different solutions to the problem. Perhaps you have to use your personal mobile phone if the company's systems are down.

Figure 22: Like in the old days



LIKE IN THE OLD DAYS

During the attack on our supplier we went back to telephone, pen and paper, like in the old days. It worked reasonably well, except that all accounting information was stored in the system.

This proactive mindset and desire to keep moving is a great asset for SMEs. Rather than waiting for external IT service providers to restore normal operations, employees wanted to help keep the business operational. With some planning and training, Swiss SMEs should be able to develop an offline workflow relying on employee cooperation, energy, and motivation. This would avoid sudden and critical stoppages in their interactions with clients and increase their ability to withstand a cyber attack.

Discussion

The employees we interviewed communicated a nuanced and differentiated set of emotions when thinking about and discussing cyber attacks. Unsurprisingly, these diverse emotions were inconsistent, yet coexisted in the minds of the group. They can be grouped into seven main themes that apply to some extent to all interviewees. Each theme has been discussed individually in Section 2. Some issues can be further differentiated by specific employee characteristics, and these are discussed in the following section. Further, we have also been able to develop actionable recommendations for SMEs and their service providers.

3.1. IMPACT BY EMPLOYEE CATEGORY

During the interviews, we noticed some additional indications of differing attitudes depending on employee category. Both the categories and the differences are purely anecdotal and reflect our observations rather than theoretical or fundamental insights. Nonetheless, we feel they offer added value to our discussion.

3.1.1. Administrative vs. Shop-Floor

The first difference we observed was between administrative, desk-bound employees and those working on the shop floor or at clients' sites. Shop-floor employees typically have only limited access to IT systems – mostly linked to manufacturing systems – and therefore, in general, feel less directly impacted by cyber attacks. Administrative employees, on the other hand, are keenly aware of the consequences of such problems. They can recall instances when their systems were down for extended periods or the impact of the attack on Meier Tobler on their own work. As a result, administrative employees should be willing to support the development of fallback processes and to practice them regularly.

3.1.2. Young vs. Old

Another potential difference – and one suggested by several interviewees – is between younger and older employees, the implication being that older people may be more vulnerable to attacks than younger ones. Younger employees were clearly more familiar with digital technology and more active on social media platforms. Older employees reported that they had not grown up with the technology and it still felt unfamiliar. Consequently, they were more cautious in their approach - possibly more aware of suspicious messages, more reluctant to engage, and more willing to ask for advice when unsure, especially in a business setting. While it is not possible to discern the actual relative risk profile, the interviewee responses suggest that these differences may not be significant. Younger employees are more familiar with the technology and hence more aware of the risks, but older employees tend to compensate for their lack of familiarity with greater caution.

3.1.3. Experts vs. Newbies

A similar but distinct potential categorization is according to the level of digital expertise. This showed some correlation with age, but very different self-described expertise levels were evident within the younger cohort. The more knowledgeable employees were also more confident about their ability to detect and recover from cyber attacks. They also tended to view any potential loss as small. Less knowledgeable employees tended to protect themselves by limiting their online exposure and only using specific platforms (e.g., e-banking) where they felt a third party provided appropriate security. While it is difficult to determine the true impact of these differences, it is not clear whether greater confidence translates into a lower potential vulnerability. Employees who, subjectively, feel more knowledgeable - and are, therefore, more confident - may engage in less risk-averse behavior expose themselves to greater danger.

3.1.4. Business vs. Personal

A further differentiation concerns individual behavior and appears to be influenced by the setting (e.g., working on the company's email system or a personal device). Interviewees stated that they were more cautious in a business setting, partly due to external/customer interactions and partly because they felt the potential for damage was greater. Business settings also tended to be more complex, with conversations often featuring the names of unknown customers and partners, again prompting greater care. Several employees mentioned fraudulent emails from fake clients or vendors, so defenses tended to be high. The interviews indicated a less vigilant approach in a personal setting. This was at least partly because respondents believed they could spot suspicious names or threads more easily and because most interviewees did not consider themselves important enough to warrant a cyber attack. This distinction may pose a threat if this more relaxed attitude is transferred to a business setting or if personal devices are breached and used to compromise business systems. The likelihood of this threat further increases when employees are regularly required to work from home, as is the case, for example, during the current corona pandemic.

3.2. RECOMMENDATIONS FOR IMPROVEMENT

Our recommendations for improvement are based on a few unambiguous observations from the interviews. In general, employees are motivated and proactive; however, they often view cyber threats as a problem for specialists. Specialists are indeed necessary, but everyone can participate in developing solutions and recovering from an attack. Furthermore, it is not clear the extent to which employees are aware of the risk and potential consequences to their organization. In light of this, we recommend three key areas for improvement. These improvements can be carried out autonomously by the companies or by service providers as part of their offering. These recommendations are complementary to the standard advice for companies to secure their infrastructure and work to mitigate the severity of potential attacks. Infrastructure should be strengthened with adequate firewalls as well as physical and password security, and an emergency response and recovery plan developed. The severity of an attack can be controlled by recognizing and protecting the company's most valuable assets, the so-called "crown jewels". These are often proprietary data, customer information, and production equipment. The recommendations from this study are designed to augment this general advice, specifically in the case of SMEs.

3.2.1. Raise Awareness

Employees seem to be aware of both the potentially catastrophic consequences of cyber attacks as well as their own vulnerability, especially to phishing attempts. At the same time, they view their company as too insignificant to warrant an attack. Cyber attacks are also considered part of a global political struggle rather than as something closer to home. Of course, this attitude is dangerous, and there are national statistics and several well-publicized cases to serve as a warning. Such information needs to be communicated directly and consistently to employees. In addition, employees should be informed regularly about the number of unsuccessful attacks on the company's IT infrastructure while being reminded of what the company is doing (e.g., upgrading firewalls) to protect itself. They also need to be reminded of the simple habits they need to adopt to reduce risk. Companies should also test their system defenses and human vulnerabilities, perhaps using ethical hackers - if they can afford the outlay - since employees are sympathetic to hackers who work for the greater good. These findings should then be communicated to employees to emphasize the importance of their role safeguarding the company.

3.2.2. Empower Employees

There is a widespread view that hackers are highly knowledgeable and well equipped, that the cyber world is complex, and that specialized service providers are the principal line of defense. While this is true to some extent, and professional service providers are part of an effective protection and response system, they cannot function in isolation. Outsourcing responsibility for cyber security to a third party invites complacency on the part of the employees, whose online behavior constitutes a vital defense line against attacks. SME employees also tend to be proactive and want to join the fight. Beyond raising awareness in their role, employees should be encouraged to participate in the discovery and communication of attacks and be recruited to develop solutions (see Section 3.2.3 below). External service providers should be asked to instruct employees and involve them as much as possible.

3.2.3. Train a Recovery Mode

In the event of an attack, or more commonly, a system malfunction, employees may not know how to respond. Their reactions, however, should not be improvised or ad-hoc. Such scenarios should be planned in advance, with supporting tools provided, and predefined triggers to emergency procedures clearly defined. Our interviews indicated that especially customer billing information and technical product specifications can be difficult to access when working offline, and this needs to be addressed carefully.

The development of a no-IT scenario can also be an opportunity for teambuilding and for leveraging the expertise of every employee. For example, companies can introduce a workshop where employees attempt to carry out their everyday jobs without regular IT tools. In this way, they will soon discover what information is vital and needs to be made available through offline systems, what tasks can be carried out on personal devices and what needs to be paper based. Such tools can then be developed during normal operations and regularly tested through “live-fire” exercises when business is conducted without the standard IT infrastructure. The recovery mode operation should have exact, predetermined triggers based on the system being affected and the outage duration.

Figure 23: Recommendations for improvement

RECOMMENDATIONS FOR IMPROVEMENT

PREPARE



RAISE AWARENESS



EMPOWER EMPLOYEES



TRAIN A RECOVERY MODE



Conclusions

Cyber attacks are a significant and growing issue, and Swiss SMEs are not an exception to this development. There has been a growth in targeted ransomware attacks in recent years. More generally, malware attacks have increasingly affected Swiss SMEs. Besides a well-conceived and up-to-date technological infrastructure, employee awareness and alert online behavior are critical components of any defense mechanism since cyber attacks typically begin with an infiltration of IT systems through phishing attacks. These attacks exploit human weaknesses to obtain passwords and other critical information. Phishing occurs almost continuously, and there is often an interval of several months between a successful phishing attempt and the actual attack, making tracing and feedback to employees difficult. The “normal” level of awareness and online behavior of employees is, therefore, the most significant indicator of vulnerability to phishing attacks

For this study, we interviewed several employees from three Swiss SMEs to understand their views on cyber attacks. Our research relied on deep metaphors to understand the emotions and the hidden drivers of employee behavior towards the threat of cyber crime. The responses were combined into common themes highlighting the broad ranges of thoughts and emotions associated with the digital world. Employees viewed cyber attacks in the broader context of global politics while recognizing the purely financial, criminal motives behind most attacks. They viewed hackers as skilled and well-equipped operatives but did not always see them as a negative force. They felt vulnerable and helpless when facing cyber attacks, and recognized the potential damage they can cause. At the same time, they tended to view their company and themselves as too small to be targeted and relied on third parties for protection in case of an attack. Fundamentally, however, they were proactive and interested in working towards practical solutions.

We have offered three actionable suggestions for SMEs to improve on existing, general recommendations for cyber security. These leverage the positive elements of the prevailing SME culture and address the riskier ones. Further information to raise awareness is necessary, as is the provision of appropriate tools, to accompany the shift towards a more direct ownership by the employees of the problems and their solutions. Further, companies need to plan for and train operations in the event of a system breakdown. Additional research should investigate whether there are any differences between employees who respond to phishing attacks and those who do not, whether employees of large organizations have similar attitudes towards cyber security, and whether the measures we suggest here mitigate the threat of cyber attacks.

References

- Allianz (2020). *Allianz Risk Barometer 2020*. (accessed 25 November 2020) <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html>
- Anz P. (2020). *Daten aus Cyber-Attacke auf Stadler Rail veröffentlicht*. (accessed 25 November 2020) <https://www.inside-it.ch/de/post/daten-aus-cyber-attacke-auf-stadler-rail-veroeffentlicht-20200529>
- Borkert S. (2020). *Bankrott auch mit Cyberangriff begründet: Wurde Mörschwiler Swisswindows in den Ruin gehackt?*. (accessed 25 November 2020) <https://www.tagblatt.ch/wirtschaft/bankrott-auch-mit-cyberangriff-begrueudet-wurde-moerschwiler-swisswindows-in-den-ruin-gehackt-Id.1198956>
- Christensen G.L. and Olson J.C. (2002). Mapping Consumers' Mental Models with ZMET. *Psychology and Marketing*, Vol. 19 (6): 477-502. doi: 10.1002/mar.10021
- Damasio A. R. (1994). Time-locked multiregional retroactivation: A systems level proposal for the neural substrates of recall and recognition. In P. D. Eimas & A. Galaburda (Eds.), *Neurobiology of cognition* (pp. 24–62). Cambridge, MA: MIT Press.
- de Moura G. et al. (2020). *Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal*. World Economic Forum (accessed 25 November 2020) <https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal>
- Dreissigacker A., von Skarczynski B. and Wollinger G.R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland*. Kriminologisches Forschungsinstitut Niedersachsen e.V., Forschungsbericht 152
- Federal Statistical Office (2020). *KMU in Zahlen*. (accessed 25 November 2020) <https://www.kmu.admin.ch/kmu/de/home/fakten-trends/zahlen-und-fakten%20/kmu-in-zahlen/firmen-und-beschaefigte.html>
- Griesser Kym T. (2020). *Nach Cyberangriff: Erpresser erhöhen Druck auf Stadler*. Tagblatt. (accessed 25 November 2020) <https://www.tagblatt.ch/wirtschaft/erpresser-erhoehen-druck-auf-stadler-Id.1235844>
- Heer A. (2020). *So greifen Cyberkriminelle Unternehmen an*. (accessed 25 November 2020) <https://www.swisscom.ch/de/magazin/datensicherheit-infrastruktur/cyberangriffe-unternehmen-malware-phishing/>
- Jochum K. (2019). *Offix von massivem Hacker-Angriff getroffen*. (accessed 25 November 2020) <https://www.inside-it.ch/de/post/offix-von-massivem-hacker-angriff-getroffen-20190703>
- Klein R. (2020). *Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite*. (accessed 25 November 2020) <https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite/>
- Lüscher A., and Niedermann M. (2019). *Hacker legen Schweizer Grossunternehmen lahm*. SRF (accessed 25 November 2020) <https://www.srf.ch/news/wirtschaft/geht-es-um-loesegeld-hacker-legen-schweizer-grossunternehmen-lahm>
- Luzerner Zeitung (2019). *Cyberattacke gegen Meier Tobler legt Betrieb weitgehend lahm*. (accessed 25 November 2020) <https://www.luzernerzeitung.ch/wirtschaft/cyberattacke-gegen-meier-tobler-legt-betrieb-weitgehend-lahm-Id.1138900>
- Mändli Lerch K. and Repic, A. (2017). *Cyberisiken in Schweizer KMUs*. (accessed 25 November 2020) https://gfs-zh.ch/wp-content/uploads/2017/12/Schlussbericht_CyberisikenKMU_12122017.pdf

- Meier Tobler (2020). *Geschäftsbericht 2019 Meier Tobler Group AG*. (accessed 25 November 2020) <https://www.meiertobler.ch/de/content/download-file/6534/file/25.02.20%20Gesch%C3%A4ftsbericht%202019.pdf>
- MELANI (2020a). *Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs*. (accessed 25 November 2020) <https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html>
- MELANI (2020b). *Semi-annual report 2020/1*. (accessed 25 November 2020) <https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2020-1.html>
- Moser S. (2019). Cyberrisiken – die unterschätzte Gefahr. *Neue Zürcher Zeitung*. 22.05.2019.
- Olson J. C., and Reynolds, T. J. (1983). Understanding consumers' cognitive structures: Implications for advertising strategy. In L. Percy & A. G. Woodside (Eds.), *Advertising and consumer psychology* (pp. 77–90). Lexington, MA: Lexington Books.
- Papedis (n. d.). *OFFIX Gruppe*. (accessed 25 November 2020) <https://www.papedis.ch/de/unternehmen/offix-gruppe/#:~:text=Mit%20einem%20Jahresumsatz%20von%20gegen,und%20Lieferanten%20in%20der%20Schweiz.>
- Pugnetti C. and Bekaert X. (2018). *A Tale of Self-Doubt and Distrust. Onboarding Millennials: Understanding the Experience of New Insurance Customers*. ZHAW School of Management and Law, ISBN 978-3-03870-021-0.
- Pugnetti C. and Schneebeli M. (2020). Kundenbedürfnisse und Marktpenetration. Schweizer KMUs unterschätzen die Bedeutung von Dienstleistungen und Versicherungsdeckungen gegen Cyberrisiken. *Schweizer Versicherung*, January 2020.
- Pugnetti C., Casián C., Staub N. and Ellenberger T. (2019). Cyber-Resilienz steigern. *Schweizer Versicherung*, October 2019.
- Schäppi M. (2020). *Cyberattacke auf Meier Tobler, Dienstleister der Gesundheitsbranche*. (accessed 25 November 2020) https://www.infosec-health.ch/Resources/Persistent/77d3731325caf3cb4a5060a02fea716d543be3c3/K_Ref2_Sch%C3%A4ppi_Cyberangriff%20auf%20DL%20der%20Gesundheitsb.pdf
- Severin C. (2019). *Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat*. (accessed 25 November 2020) https://www.offix.ch/media/cms/Offix/Media/NZZ_Cyber-Angriff%20auf%20KMU_OFFIX-Gruppe.pdf
- SIA (2018). *Grundlagenpapier des SVV zu Cyber-Risiken*. Arbeitsgruppe Cyber-Risk, Swiss Insurance Association (accessed 25 November 2020) https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf
- SRF (2020). *Offenbar zwang eine Cyberattacke Swissswindows in die Knie*. (accessed 25 November 2020) <https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swissswindows-in-die-knie>
- Stadler Rail (2020a). *Geschäftsbericht 2019*. (accessed 25 November 2020) https://www.stadlerrail.com/media/pdf/web_stadler_rail_gb19_de.pdf
- Stadler Rail (2020b). *Cyber-attack against Stadler IT network*. (accessed 25 November 2020) https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf
- Trustwave (2020). *2020 Trustwave Global Security Report*. (accessed 25 November 2020) <https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/>

Zaltman G. (1997). Rethinking Marketing Research: Putting People Back In. *Journal of Marketing Research*, Vol. 34, 4. <https://doi.org/10.1177/002224379703400402>.

Zaltman G. and Zaltman L. (2008). *Marketing Metaphoria: What Deep Metaphors Reveal about the Minds of Consumers*. Harvard Business Press.

Tables

Table 1: Current cyber insurance coverages	9
Table 2: Research question	11
Table 3: Self-description of interviewees	11
Table 4: Common themes and picture labels	12

Figures

Figure 1: Estimated yearly rate of cyber attacks on SMEs	7
Figure 2: Secret service	13
Figure 3: Man in the shadow	13
Figure 4: The loot	13
Figure 5: The hacker	14
Figure 6: Cool working space	14
Figure 7: Villain or benefactor?	14
Figure 8: Data magnet	15
Figure 9: Social manipulation	15
Figure 10: Unanswered questions	15
Figure 11: Surveillance	16
Figure 12: Be careful!	16
Figure 13: Phishing	16
Figure 14: Modern breaking and entering	17
Figure 15: Attack on our supplier	17
Figure 16: I hope not!	17
Figure 17: The whole world	18
Figure 18: Fear	18
Figure 19: Personal support	18
Figure 20: Fog	19
Figure 21: Planning	19
Figure 22: Like in the old days	19
Figure 23: Recommendations for improvement	22

Authors



Dr. Carlo Pugnetti is a Lecturer at the Institute for Risk & Insurance at ZHAW. His research focuses on the evolution of customer behavior in insurance, with a particular focus on the changes triggered by technology adoption and generational differences. He is also exploring the connection between innovation and risk management.

Prior to joining ZHAW, Carlo served as CEO of Allianz Global Assistance in Switzerland and in several other functions within the Allianz Group - restructuring the Claims Department at Fireman's Fund in the United States, on strategic issues in Group Development in Munich, and leading an international Line of Business in Paris. Carlo began his career as a consultant for Oliver Wyman.

Carlo holds a Ph.D. in Risk Analysis and a Master's degree in Electrical Engineering, both from Stanford University.



Carlos Casián is Underwriter for Property and Cyber Risk at Allianz Suisse. He has led internal and external training programs and has participated in several expert panels. He is a public speaker for Allianz Suisse on cyber risks and represents the company in the Working Group Cyber Risk at the Swiss Insurance Association.

Carlos learned insurance from the ground up, beginning his career with Allianz Suisse more than a decade ago. In recent years, he has focused on cyber risks and their impact on company risk profiles.

Carlos holds a BSc in Business Administration with a specialization in Risk & Insurance from ZHAW.

Partners

Our sincere thanks to our partner companies, who provided access to their employees and supported the study.



Kurt Wyss, Partner
VTL Insurance + Partner AG



www.vtl.ch



Sokol Prendi, Head of Sales
Dätwyler Fertigungs-Technologie AG



www.daetwylerag.ch



Manuel Fischer, CEO
Fischer Wärmetechnik AG



www.heizprofi.ch



Terence Iseli, CEO
ISELI ENERGIE AG



www.iseli-energie.ch



Xavier Bekaert, Partner
Benthurst & Co.



www.benthurst.com

School of Management and Law

St.-Georgen-Platz 2
P.O. Box
8401 Winterthur
Switzerland

www.zhaw.ch/sml



AACSB
ACCREDITED

swissuniversities